UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/472,752	05/16/2012	Eric F. LE SAINT	AIM-211CON2	8428

101221 7590 04/27/2017
Muirhead and Saturnelli, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581

EXAMINER
NGUYEN, TU X

ART UNIT	PAPER NUMBER
2649	

MAIL DATE	DELIVERY MODE
04/27/2017	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte ERIC F. LE SAINT and
DOMINIQUE LOUIS JOSEPH FEDRONIC

Appeal 2017-003100
Application 13/472,752[1]
Technology Center 2600

Before HUNG H. BUI, ADAM J. PYONIN, and JOSEPH P. LENTIVECH, *Administrative Patent Judges*.

BUI, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of claims 1, 40–43, and 45–48, which are all the claims pending in the application. Claims 2–39 and 44 are cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.[2]

[1] According to Appellants, the Real Party in Interest is Assa Abloy AB. App. Br. 2.

[2] Our Decision refers to Appellants' Appeal Brief filed December 11, 2015 ("App. Br."); Examiner's Answer mailed May 20, 2016 ("Ans."); Final Office Action mailed May 8, 2015 ("Final Act."); and original Specification filed May 16, 2012 ("Spec.").

STATEMENT OF THE CASE

Appellants' Invention

Appellants' invention relates to "an intelligent remote device equipped with a security token which emulates a local security device peripheral in a peer-to-peer relationship over a private network without reduction in the overall level of security." Spec. 3:16–19. According to Appellants, "the intelligent remote device includes a personal data assistant (PDA), a cellular telephone having private networking capabilities, a network appliance or a personal security device such as a secure PIN pad." Spec. 3:19–22. The "security token" is a hardware based security device such as a subscriber identification module (SIM). Spec. 3:25–26.

> "Once the communications connection is established [between an intelligent remote device and a host site of a private network], a critical security parameter (CSP) associated with a user is provided to the security token using the intelligent remote device as a communications interface. A critical security parameter as defined herein includes authentication data, passwords, PINs, secret and private cryptographic keys."

Spec. 4:21–25.

Independent claim 1 is illustrative of Appellants' invention and is reproduced below with disputed limitations in italics:

> 1. A method for accessing a security token enabled computer system, comprising:
>
> establishing a wireless communications connection between an intelligent remote device and the security token enabled computer system;

> *providing a critical security parameter associated with a user to a security token operatively coupled to the intelligent remote device;*
>
> *authenticating the critical security parameter using the security token; and*
>
> *sending an access request message to the security token enabled computer system to invoke establishment of a secure communications connection between the security token and the security token enabled computer system, wherein the access request message identifies the security token.*

App. Br. 13 (Claims App'x).

Examiner's Rejections and References

(1) Claims 1, 40, 45, 46, and 48 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Flodén et al. (US 6,230,002 B1; issued May 8, 2001; "Floden"). Final Act. 3–4.

(2) Claims 41 and 42 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Floden and Audebert et al. (US 2002/0194499 A1; published Dec. 19, 2002; "Audebert"). Final Act. 5.

(3) Claim 43 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Floden and Mizrah (US 2005/0050323 A1; published Mar. 3, 2005). Final Act. 5–6.

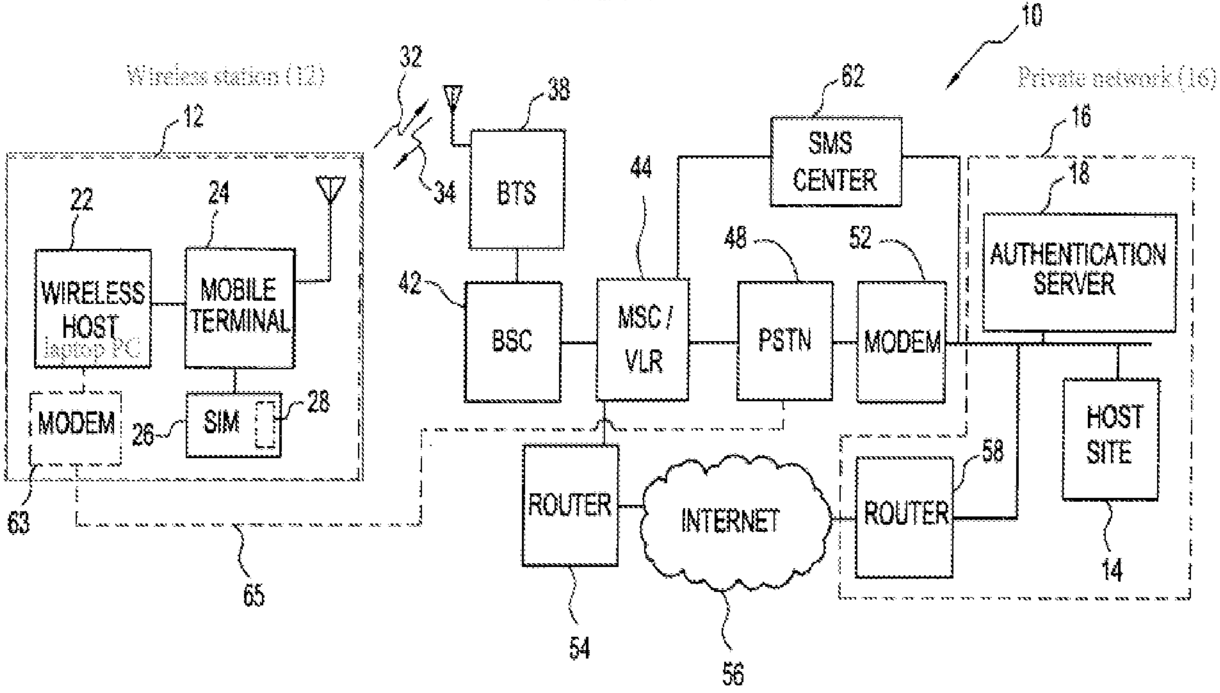
(4) Claim 47 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Floden and Audebert et al. (US 2002/0162021 A1; published Oct. 31, 2002; "Audebert '021"). Final Act. 6.

ANALYSIS

§ 102(b) Rejection of Claims 1, 40, 45, 46, and 48 based on Floden

With respect to independent method claim 1, the Examiner finds Floden discloses Appellants' claimed "method for accessing a security token enabled computer system" comprising: "establishing a wireless communications connection between an intelligent remote device and the security token enabled computer system" in the form of wireless communications between (1) mobile terminal 24 having SIM card 26 of wireless station 12 and (2) host site 14 of private network 16 having authentication server 18, shown in Figure 1, as reproduced below with additional markings for illustration:

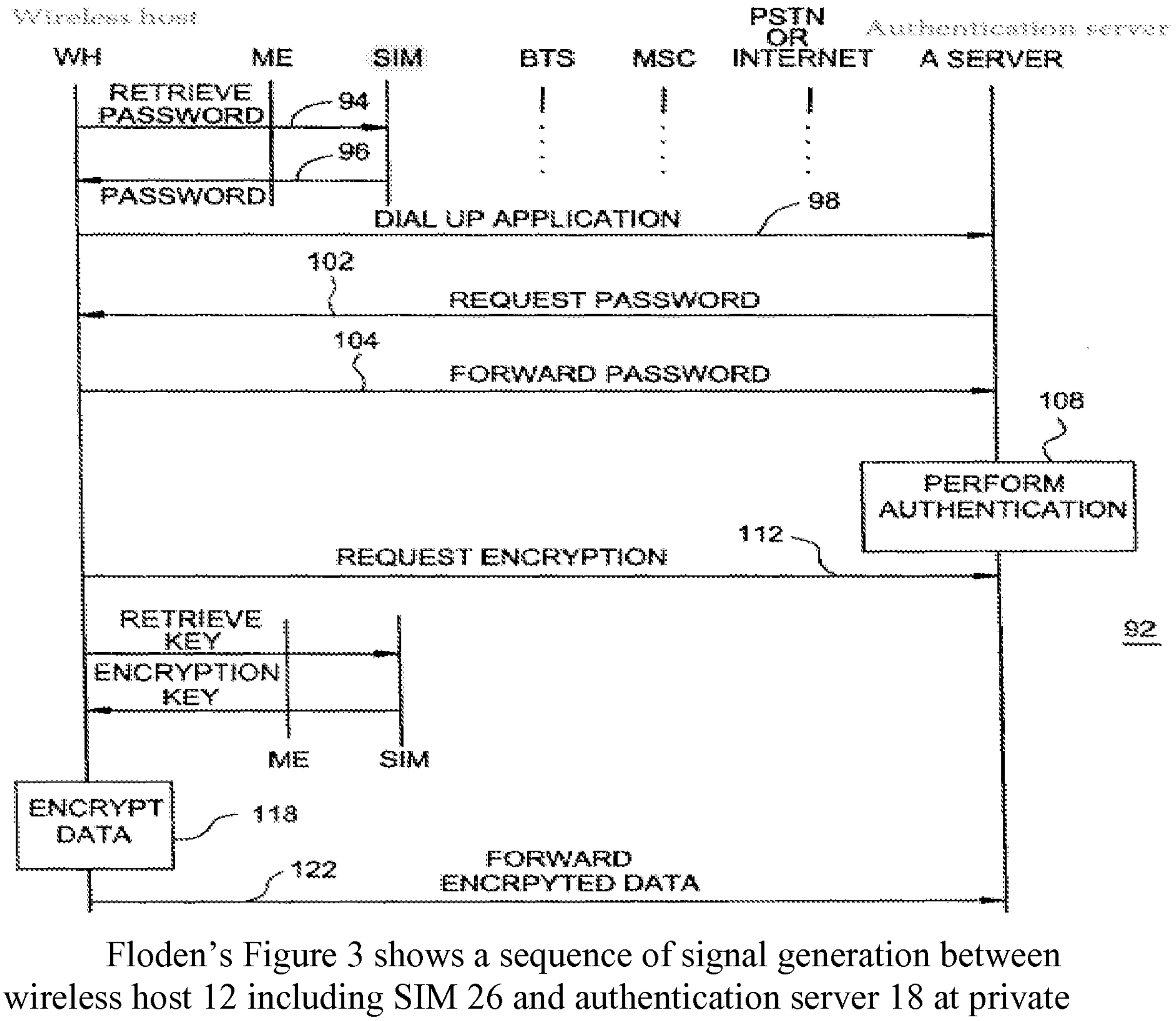
FIG.1



Floden's Figure 1 shows wireless communications between (1) mobile terminal 24 having SIM card 26 of wireless station 12 and (2) host site 14 of private network 16 having authentication server 18.

The Examiner also finds Floden discloses: (1) “providing a critical security parameter associated with a user to a security token operatively coupled to the intelligent remote device” and (2) “authenticating the critical security parameter using the security token” in the form of password 64 provided to SIM 26, shown in Floden’s Figure 3. Final Act. 3 (citing Floden 7:32–35). Floden’s Figure 3 shows a sequence of signal generation between wireless host 12 including SIM 26 and authentication server 18 at private network 16, as reproduced below with additional markings.

FIG.3



Floden’s Figure 3 shows a sequence of signal generation between wireless host 12 including SIM 26 and authentication server 18 at private network 16.

The Examiner further finds Floden discloses "sending an access request message to the security token enabled computer system to invoke establishment of a secure communications connection between the security token and the security token enabled computer system, wherein the access request message identifies the security token" in the form of dial-up request 98 sent to authentication server 18 and password 104 forwarded to authentication server 18, shown in Floden's Figure 3. Final Act. 3 (citing Floden 7:38–45).

Appellants dispute the Examiner's factual findings regarding Floden. First, Appellants argue Floden does not teach "providing a critical security parameter associated with a user to a security token operatively coupled to the intelligent remote device" as recited in claim 1. App. Br. 7–8. In particular, Appellants acknowledge Floden teaches "a password that is generated within the SIM," but argue Floden's "password generated at the SIM" is "provided without regard to a user, but rather based on an algorithm that is mirrored at the authentication server of Floden to obtain authentication." App. Br. 7 (citing Floden 6:49–7:26, 8:63–9:9).

Second, Appellants argue Floden does not teach "authenticating the critical security parameter using the security token" as recited in claim 1. App. Br. 8. In particular, Appellants acknowledge "Floden discusses using an authentication server to authenticate a password obtained from a SIM device permitting a wireless host to access a host site of a private network." App. Br. 8 (citing Floden 7:16–26). However, Appellants argue such authentication occurs at an authentication server, and not at the SIM device.

Id. According to Appellants, "no authentication is actually performed at the mobile terminal, or the wireless host." *Id.* at 8 (citing Floden 2:64–3:5).

Third, Appellants argue Floden does not teach "sending an access request message to the security token enabled computer system to invoke establishment of a secure communications connection between the security token and the security token enabled computer system, wherein the access request message identifies the security token" as recited in claim 1. App. Br. 8–9. Appellants acknowledge "Floden discusses the use of an encryption key to encrypt information that is communicated from the wireless host to the host site." App. Br. 8 (citing Floden 3:33–37, 4:7–14). However, Appellants argue "it is the wireless host of Floden that is involved in encrypted communication with the host site of the private network, not the SIM or the mobile terminal." *Id.* at 8 (citing Floden 7:60–67).

We do not find Appellants' arguments persuasive. Nor do we find these arguments commensurate with the scope of claim 1. Instead, we find the Examiner has provided a comprehensive response to Appellants' arguments supported by a preponderance of evidence. Ans. 2–3. As such, we adopt the Examiner's findings and explanations provided therein. *Id.* At the outset, we note there is no requirement that the prior art must use the same words to describe a claim element in order to be deemed as teaching or disclosing that claim element. "[T]he reference need not satisfy an *ipsissimis verbis* test," i.e., identity of terminology is not required. *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009). Prior art references must be "considered together with the knowledge of one of ordinary skill in the pertinent art." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

As correctly recognized by the Examiner, Floden discloses the password (i.e., Appellants' claimed "critical security parameter associated with the user" is provided at the mobile terminal's SIM (i.e., Appellants' claimed "security token"), shown in Floden's Figure 3. Ans. 2 (citing Floden 6:55–56). Nevertheless, Appellants continue to argue that:

> "the password of Floden is generated at the mobile terminal to provide and store in a SIM card (security token), and thus is associated with the device, not necessarily any particular user. If a plurality of different users used the same device they would all, in effect, share the same 'password' under the teachings of Floden."

Reply Br. 3–4.

We disagree. Each SIM card 26, as shown in Floden's Figure 1, is a subscriber identity module (SIM) uniquely assigned to a subscriber (user) and, as such, any "password" generated by SIM card 26 is "associated with the user" in the manner recited in Appellants' claim 1. *See* Floden 2:27–41.

Appellants' remaining arguments are not commensurate with the scope of claim 1. For example, claim 1 only requires "authenticating the critical security parameter using the security token" and does not require such an authentication to occur at authentication server 18, shown in Figures 1 and 3, or to occur as part of password retrieval from SIM card 26, shown in Figure 3. As such, Appellants emphasis that "the SIM does not actually perform any authentication" is not persuasive. Reply Br. 4. As recognized by the Examiner, "the actual acquiring of the generated password from the mobile terminal is considered part of the initial authentication process as this is an important needed step in the process." Ans. 3.

Based on this record, we are not persuaded of Examiner error. Accordingly, we sustain the Examiner's anticipation rejection of independent claim 1 and its dependent claims 40, 45, 46, and 48, which Appellants do not argue separately. App. Br. 9.

With respect to the remaining claims 41–43 and 47, Appellants reiterate the same arguments presented against claim 1. App. Br. 12. For the same reasons discussed, we sustain the Examiner's obviousness rejection of claims 41–43 and 47.

CONCLUSION

On the record before us, we conclude Appellants have not demonstrated the Examiner erred in rejecting claims 1, 40–43, and 45–48 under 35 U.S.C. § 102(b) and § 103(a).

DECISION

As such, we AFFIRM the Examiner's Final Rejection of claims 1, 40–43, and 45–48.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED